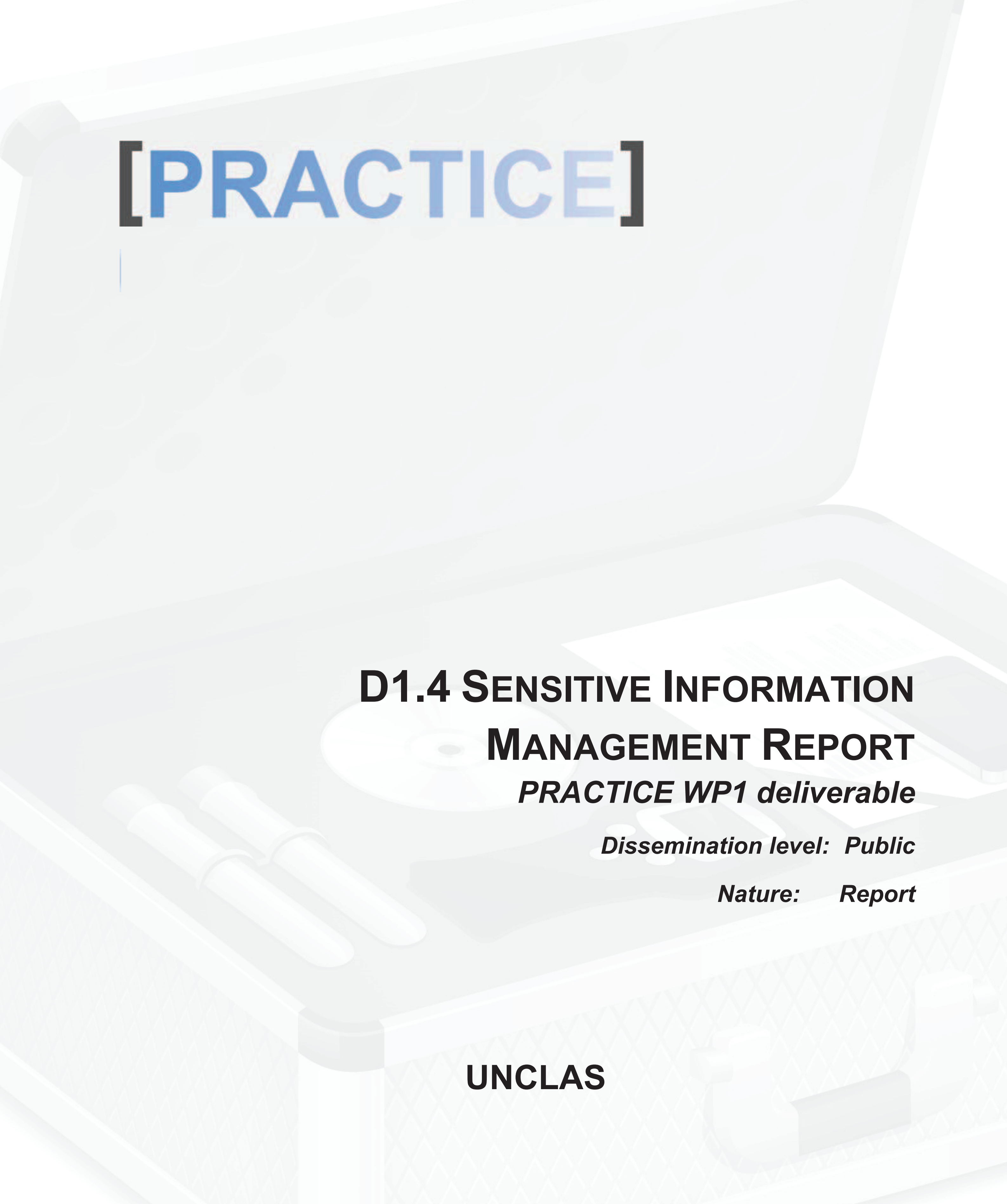

[PRACTICE]

D1.4 Sensitive Information Management Report

PRACTICE WP1 deliverable

Dissemination level: Public

Nature: Report

UNCLAS

SEVENTH FRAMEWORK PROGRAMME

Preparedness and Resilience Against CBRN Terrorism using Integrated Concepts and Equipment
practice-fp7-security.eu

1. Executive Summary

This report describes the work of the Security Scrutiny Committee that warranted that PRACTICE deliverables, reports and publications do not contain security sensitive information. The Security Scrutiny Committee consisted of three members, who all have long experience in handling classified information and of working under national security clearance conditions. The Security Scrutiny process was a combination of re-active and pro-active work to ensure that no sensitive information is present in any public material generated in the PRACTICE project. Only three deliverables (D2.2, D2.3 and D6.2) have contained sensitive information and have been modified accordingly.

2. Security Scrutiny Committee

It was the task of the **Security Scrutiny Committee** to warrant that project deliverables, reports and publications do not contain security sensitive information. PRACTICE was a public project and the majority of deliverables are open to stakeholders and the interested public in general. The Security Scrutiny Committee consisted of three members, who all have long experience in handling classified information and working under national security clearance conditions:

- Dr. Maarten Nieuwenhuizen (TNO)
- Dr. Hans Christian Gran (FFI),
- Dr. Ola Claesson (FOI, chair, from the start of the project until April 2012),
- Dr. Agneta H. Plamboeck (FOI, chair from April 2012 until end of project)

3. Security scrutiny process

A **security scrutiny process** was established in which the three security experts individually and independently reviewed each draft deliverable. They were to agree unanimously on the security status of each deliverable and – where necessary – to censor sensitive information. For each deliverable the review process concluded with a security decision according to a common format, in which the committee either declared its formal approval or demanded specific changes (Annex I). Only after removal or censoring of the sensitive information the deliverable was submitted to the EC and published on the project website. Security sensitive material, deemed by the committee to be exempted from public disclosure, is kept by the lead beneficiary responsible for a deliverable. This material is available to consortium members and the EC upon request. In case of security issues with a deliverable, the project manager informed the EC Project Officer.

Given the numerous deliverable deadlines and occasional delays in deliverable production, live meetings for the purpose of security decisions on deliverables were not practical. The committee members therefore performed a remote review and communicated within the group via a dedicated internal web portal. Security decision forms are archived by the project manager. We found this remote security scrutiny procedure to work well.